

Secure Naming Infrastructure Pilot (SNIP)

A .gov Community Pilot for DNSSEC Deployment

GovSec 2009, March 12th

Scott Rose, NIST

scottr@nist.gov

SNIP Goals

- **DNSSEC is now a FISMA Requirement and OMB Mandate.**
 - NIST SP-800-53 (r3 issued in Feb 2009) mandates the incremental deployment of DNSSEC at all levels.
 - Low/Moderate/High Impact – must sign zones.
 - High Impact – must be prepared to validate signatures.
 - OMB M-08-23 mandate deadlines sync with FISMA deadlines
- **Need to facilitate technology insertion and adoption.**
 - Standards, implementations and policies don't guarantee success.
 - Need for technical community resources and activities to foster early deployments, refine policies and plans, share information and expertise.

SNIP Basics

- SNIP will build a USG DNS Ops community and shared pilot
 - Provide “distributed training ground” for .gov operators deploying DNSSEC
 - Ability to pilot agency specific scenarios either locally or in SNIP-provided resources.
 - Create a community resource for DNS admins in the USG to share knowledge and to refine specifications, policies and plans.
- SNIP basis is a signed shadow zone under .gov (dnsops.gov)
 - Will offer delegations and secure chaining to subzones
 - example – NIST would participate as nist.dnsops.gov

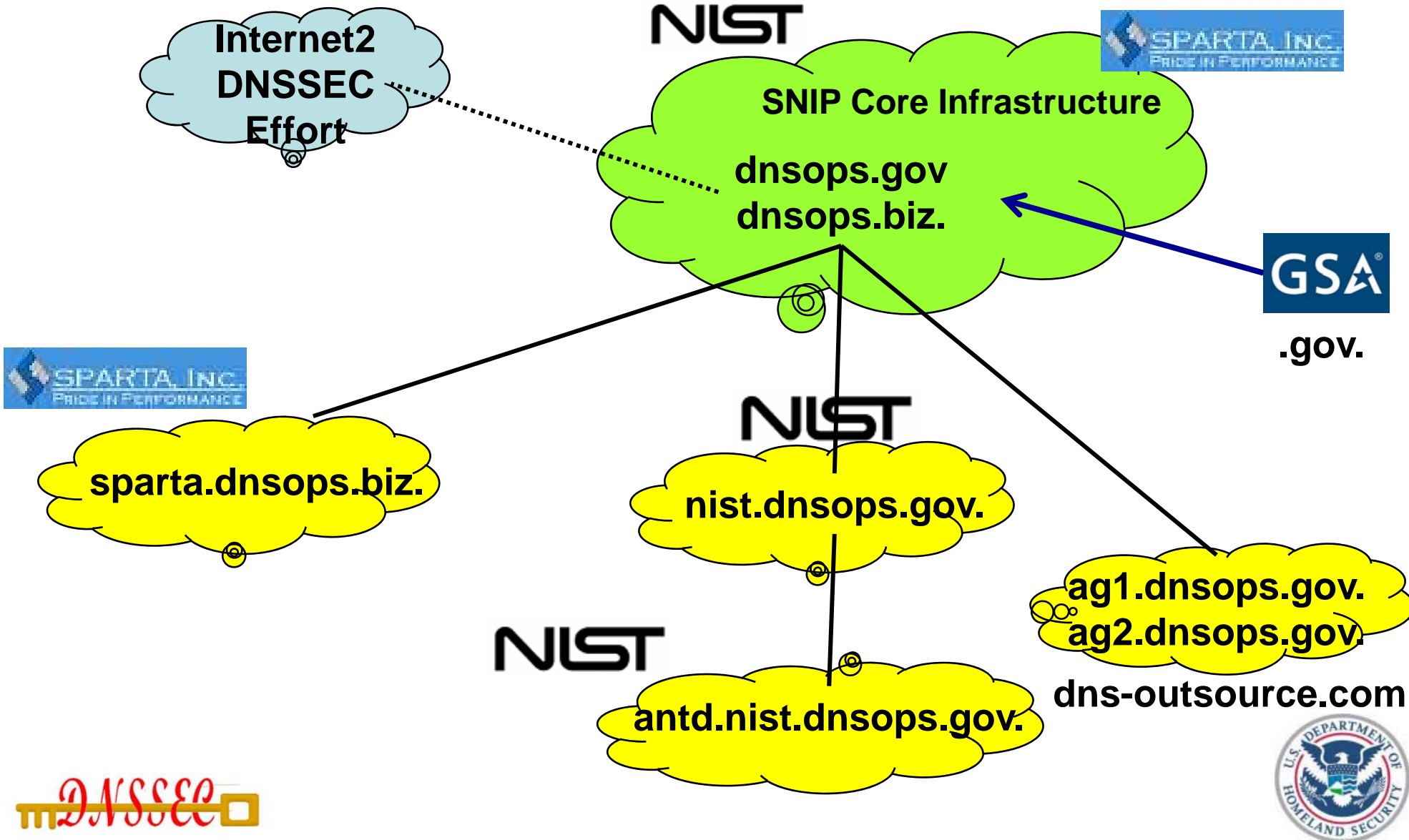
What SNIP is Not

- Mandatory
- Permanent
 - Expected lifetime: 2-3 years from start (in 2nd year now)
 - The community tools and email lists will remain after the testbed activities conclude..
- 100% Uptime
 - This is a experimental testbed in which we will conduct disruptive experiments, load/stress test servers, etc.

SNIP as a Testbed

- Use SNIP tree to exercise DNSSEC operations
 - Test deployment DNSSEC scenarios.
 - Multi-vendor platforms for authoritative / caching servers, resolvers.
 - Zone structure / contents / distribution.
 - Test DNSSEC operations described in SP800-81
 - Zone signing, key rollovers, zone transfers.
 - Test DNSSEC implementations and administration tools
 - Test performance – in agency specific scenarios.
- Community hands-on participation
 - Agency DNS operators can participate in NIST/SPARTA led exercise.

The Big Picture – DNSSEC in .gov



DNSSEC-Deployment.org

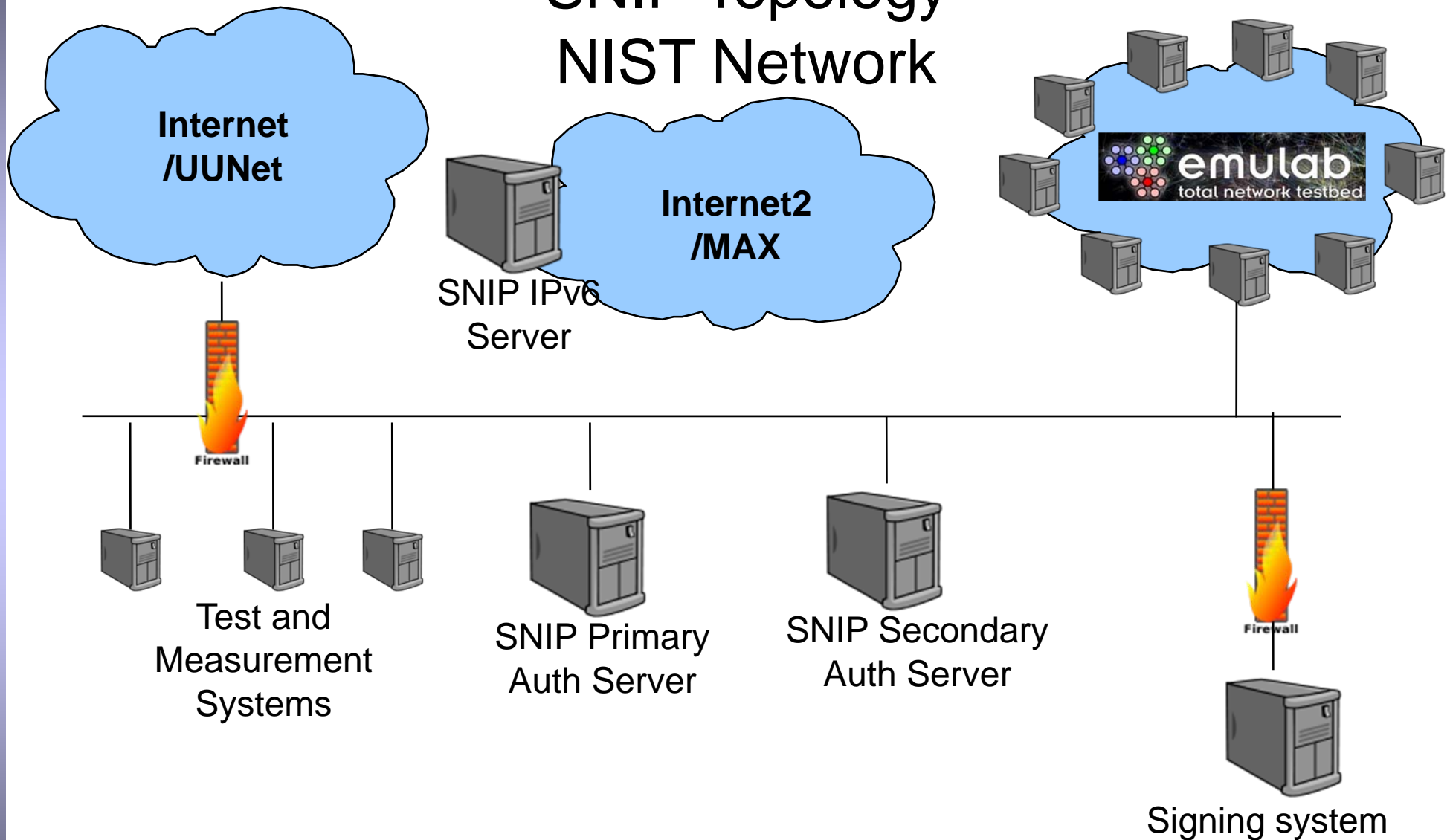
Testbed Technical Details

- Multiple authoritative server implementations
- Internet2 connection (IPv6 testing)
- May have alternate hosting capabilities (multiple servers)
- Maintain and publish trust anchor for dnsops.gov/biz.tree

SNIP Infrastructure Resources

- Primary Site – NIST / Gaithersburg MD.
 - Authoritative dnsops.gov and dnops.biz DNS servers
 - Also home of implementation test systems
- Secondary Site – Sparta / Columbia MD
 - Geographic and network dispersion (sort of)
 - Zone transfers using TSIG for message authentication
- Signing Infrastructure – dnsops.gov. apex.
 - Done behind firewall at NIST
 - Private keys not stored on servers

SNIP Topology NIST Network



SNIP Operational Overview

- Will use procedures outlined in SP800-81
 - 1024 bit RSA ZSK
 - Rolled over every month
 - 2048 bit RSA KSK – “Trust Anchor”
 - Rolled over during experimentation
- ZSK rollover every 30 days
 - KSK on a less formal basis (currently 1 year)
- Using NSEC
- These parameters will change as Federal Guidelines change

SNIP Impact

- **Stepping stone for operational use**
 - USG DNS operators get experience running delegation under dnsops.gov before deploying in own agency
- **Tool testing**
 - Tech transfer / training on existing tool suites (NIST, SPARTA, Shinkuro, ISC, et al).
- **Platform Testing**
 - Multi-vendor environment
 - Servers - ISC/BIND, NSD, Secure64, Windows Server 2008 R2 and more...
 - Resolvers – Linux, BSD, Microsoft, OS X.
- **Procedure Testing**
 - Refinement of procedure/policy guidance and reporting requirements
 - All results will form the basis of NIST SP 800-81r1

Participation

- Will try to accommodate all
 - Non USG entities: dnsops.biz
 - Tool developers
 - Can run locally or have delegation/secondary/etc as necessary.
- Two ways to join:
 - Using the dotgov.gov interface for those with logins
 - Similar to actual production interface with the .gov TLD
 - Participation page on project webpage

Resources

- SNIP Project Page
<http://www.dnsops.gov/>
- DNSSEC-Deployment Web page
 - Informal working group<http://www.dnssec-deployment.org/>